AO 106 (Rev. 04/10) Application for a Search Warrant

FILED

UNITED STATES DISTRICT COURT

for the

Western District of Texas

2012 DEC 18 PM 1:52

CLERK US DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY _____ DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Network Investigative Technique (NIT) for e-mail address 512SocialMedia@gmail.com

Case No. A12-M-748

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See "Attachment A"

located in the State and District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. § 1344	Bank Fraud

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Justin E. Noble, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12-18-2012

Judge's signature

City and state: Austin, Texas

Mark P. Lane, United States Magistrate Judge
Printed name and title

Attachment A

Place to Be Searched

The portion of the computer activating the network investigative technique ("NIT") that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

Attachment B

Things To Be Seized

Information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section 1038 of Title 18, United States Code (False information and hoaxes). This information may include environmental variables and/or certain registry-type information, such as:

A. The computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

B. The computer's MAC address. Each time a computer communicates over a local area network (or "LAN"), it uses a hardware device called a network interface card. Manufacturers of network interface cards assign each one a unique numeric identifier called a media access control or "MAC address."

C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

D. A list of programs running on the computer.

E. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Vista), and serial number.

F. The web browser and version running on the computer. The web browser is the program that allows user to view web pages. Firefox, Internet Explorer, Netscape, Opera and Safari are examples of web browsers.

G. The computer's language encoding and default language. Users can set computers to display text in a particular language.

H. The computer's time zone information.

I. The registered computer name and registered company name. Users generally input this information when the computer is first purchased.

J. The current logged-in user name and list of user accounts.

K. The computer's wired and wireless network connection information, dial-up account information, and trace-route information. This information identifies the way that the computer is connected to the Internet.

L. The Uniform Resource Locator ("URL") to which the target computer was previously connected. URLs, such as www.uscourts.gov, are used to access web sites.

M. Other similar identifying information on the activating computer that may assist in identifying the computer, its location, other information about the computer, and the user of the computer may be accessed by the NIT.

AFFIDAVIT OF JUSTIN E. NOBLE
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Justin E. Noble, being first duly sworn, hereby depose and state as follows:

A. Introduction and Affiant Background

1. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT"). I request approval to send one or more communications to 512SocialMedia@gmail.com. Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. There is probable cause to believe that a federal fugitive, namely Donald Lee Phelps, is using the email address 512SocialMedia@gmail.com (target email). On October 16, 2007, Phelps was indicted by a Federal Grand Jury in the Northern District of Florida for a violation of 18 U.S.C. § 1344. Affiant believes that evidence relating to Phelps's location exists on the computer that will receive the NIT described above.

2. I have been a FBI Special Agent since August 2007 and have been assigned to the San Antonio Office's Austin RA since May 2011. I have primarily investigated violent crime, drugs, and criminal enterprise matters. I am familiar with the habits and practices of fugitives from justice. I have participated in federal investigations which have utilized telephone wire interceptions, telephone toll analysis, undercover operations, search and seizure warrants, surveillance, intelligence analysis, interviews and interrogations, and the review of financial documents. I have searched residences for items related directly and indirectly to fugitive matters. Due to my training and experience, I am familiar with fugitive's methods of concealment and efforts to avoid prosecution, custody, and/or confinement.

3. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

B. Probable Cause

4. Donald Lee Phelps is wanted for his alleged involvement in a scheme to defraud financial institutions. From 2005 through 2006, Phelps allegedly assumed the identity of his girlfriend's estranged husband who was deployed with the U.S. military in Iraq. Using an altered Texas driver's license, Phelps obtained a Florida ID using the assumed name. Using this identity, Phelps is alleged to have established accounts at a credit union, gained employment at a computer learning center, and received a regular salary. Phelps also wrote personal checks for all of his expenses, obtained loans, credit cards, and sought medical care under this false name. On October 16, 2007, a federal warrant was issued for Phelps's arrest, charging him with bank fraud. I also know that Phelps is wanted on unrelated but similar charges in Pennsylvania, Arizona and Texas.

5. On November 14, 2012, a confidential human source (CHS #1) provided 512.468.0748 (TT #1) as a contact number for Phelps. CHS #1's information has been corroborated and deemed reliable and credible based upon an independent investigation by the Austin Police Department, Round Rock Police Department, and the FBI. A check of CHS #1's criminal history revealed no felony convictions.

6. CHS #1 advised that Donald Lee Phelps has been residing in and around Austin, Texas, for the past five years. He works as computer programmer and operates a business called Extreme Social Media (ESM) under the assumed name of James Bridges. According to CHS #1, Phelps routinely colors his facial hair and wears a toupee. CHS #1 has had regular and frequent contact with Phelps since 2007 and positively identified Phelps from a photograph. CHS #1 used TT #1 to make regular contact with Phelps. The last contact that the CHS had with Phelps on TT #1 was on November 15, 2012.

7. On November 20, 2012, U.S. Magistrate Judge Andrew W. Austin signed a search warrant authorizing Agents to geo-locate TT #1. On November 21, 2012, at approximately 11:55 a.m., agents obtained a single location for TT #1. The obtained location suggested that TT #1 was located at a Drury Inn Hotel in San Antonio, Texas. At approximately 3:00 p.m., agents arrived at the Drury Inn Hotel. Hotel staff positively identified a photograph of Phelps as being a patron of the hotel. Hotel staff advised that Phelps checked out of his room on November 21, 2012, at approximately 2:00 p.m. Phelps had been staying at the hotel under the assumed name, Jack Rady, and used cash to pay all hotel costs.

8. On December 3, 2012, affiant learned that email address, JBridges007@gmail.com, was used as contact email for Phelps. On December 4, 2012, affiant served a Federal Grand Jury (FGJ) subpoena to Google requesting internet protocol (IP) addresses used to access JBridges007@gmail.com. On December 4, 2012, research on the Google returned IP addresses revealed that an IP anonymizer, namely HideMyAss.com, was being used to mask the true IP addresses being used to access the JBridges007@gmail.com.

9. On December 11, 2012, a confidential human source (CHS #2) provided email address 512SocialMedia@gmail.com as a contact email address for Phelps. CHS #2 also provided Amplify Credit Union (ACU) account number 4474228 as a checking account used by Phelps. CHS #2's information has been corroborated and deemed reliable and credible based upon an independent investigation by the Austin Police Department, Round Rock Police Department, and the FBI. A check of CHS #2's criminal history revealed no felony convictions.

10. Affiant contacted ACU and learned that account number 4474228 was a business account used by ESM. The account was currently overdrawn and had not been used since November 12, 2012. On December 8, 2012, an individual accessed the account via the internet. Research on the IP address used to access the ACU account revealed that HideMyAss.com was used to mask the true IP address of the individual attempting to access the account.

11. CHS #2 positively identified a photograph of Phelps as being the user of email account 512SocialMedia@gmail.com. Phelps used 512SocialMedia@gmail.com to make contact with CHS #2 on December 10, 2012.

12. Based on the facts, probable cause exists to believe that a NIT sent to the 512SocialMedia@gmail.com will reveal evidence of Phelps's location, such as the location of the computer expected to receive the NIT and true IP addresses used to access the target email address.

C. Place to be Searched and Property to be Seized

13. If a computer successfully activates the NIT, the NIT will conduct a one-time limited search of that computer. The NIT utilizes computer instructions to cause an activating computer to send certain information to a computer controlled by the Federal Bureau of Investigation, which will assist FBI's Austin RA in the forensic aspects of this investigation.

14. The NIT is designed to collect the items described in Attachment B – *i.e.*, information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of Phelps location, a fugitive who is wanted for violations of Section 1344 of Title 18, United States Code (Bank Fraud). This information may include the portion of the activating computer that contains environmental variables and/or certain registry-type information, such as:

A. The computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

B. The computer's MAC address. Each time a computer communicates over a local area network (or "LAN"), it uses a hardware device called a network interface card. Manufacturers of network interface cards assign each one a unique numeric identifier called a media access control or "MAC address."

C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

D. A list of running programs running on the computer.

E. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Vista), and serial number.

F. The web browser and version running on the computer. The web browser is the program that allows user to view web pages. Firefox, Internet Explorer, Netscape, Opera and Safari are examples of web browsers.

G. The computer's language encoding and default language. Users can set computers to display text in a particular language.

H. The computer's time zone information.

I. The registered computer name and registered company name. Users generally input this information when the computer is first purchased.

J. The current logged-in user name and list of user accounts.

K. The computer's wired and wireless network connection information, dial-up account information, and trace-route information. This information identifies the way that the computer is connected to the Internet.

L. Uniform Resource Locator ("URL") to which the target computer was previously connected. URLs, such as www.uscourts.gov, are used to access web sites.

M. Other similar information on the activating computer that may assist in identifying the computer, its location, other information about the computer, and the user of the computer may also be accessed by the NIT.

15. Each of these categories of information sought by the NIT may contain evidence of the crime under investigation, including information that may help to identify the computer receiving the NIT and its user. The computer's true assigned IP address can be associated with an Internet service provider ("ISP") and a particular ISP customer. The MAC address is unique to a specific computer on a network. A list of open communication ports and running programs can corroborate whether the NIT is reading the correct computer by showing whether that computer is using the world wide web, sending and receiving emails, or reading attachments. The operating system and browser types and versions can also corroborate the identity of a computer and, in the case of an operating system's serial number, can provide evidence to identify the user because corporations maintain databases of purchasers of their operating systems. The language encoding and computer default language can help identify the subject by identifying his native spoken language. The computer name, company name, logged-in user name can identify the network, specific computer on a network, and perhaps even the name of the person(s) who use the computer. Trace-route information can help identify where on a

network or even where physically a computer may be located. Wireless network connection information can tell from where a computer accessed the Internet, even if it was through the unauthorized use of a wireless network (a technique used by Internet criminals). Wired network information and dial-up account information can help identify what computer was used to access the Internet to receive the NIT. Time zone information will assist in confirming the geographical location of the subject computer. The last-visited URL can sometimes help corroborate the identity of the computer and user by, for example, showing that the NIT ran after the user visited the web-based e-mail server for the target email address.

16. Based on my training, experience, and the investigation described herein, I know that network level messages and information gathered directly from a sending computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. Getting IP address and other information directly from the computer being used by the subject can defeat such techniques.

17. The NIT will cause the above-described information to be sent over the Internet to a computer controlled by the FBI, located in Quantico, Virginia, located in the Eastern district of Virginia, and then be relayed to the investigators in the Western District of Texas who will analyze the resulting information.

18. Based upon the information above, I have probable cause to believe that Donald Lee Phelps uses 512SocialMedia@gmail.com and that the computer that receives the NIT will be used by Phelps. I further submit that there is probable cause to believe that using a NIT in conjunction with the target address will assist in identifying the activating computer, its location

and the location of Phelps. By this affidavit and application, I request that the Court issue a search warrant authorizing the use of the NIT described herein.

19. Because notice as required by Rule 41(f)(3) of the Federal Rules of Criminal Procedure would jeopardize the success of the investigation, and because the investigation has not identified an appropriate person to whom such notice can be given, I hereby request authorization to delay such notice for 30 days from the sending of the NIT.

20. Because there is legitimate law enforcement interests that justify an unannounced use of the NIT and review of the messages generated by the activating computer in this case, I ask this Court to authorize the proposed use of a NIT without the prior announcement of its use. One of these legitimate law enforcement interests is that announcing the use of the NIT would assist a person using the activating computer to defeat the activation of the NIT.

21. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) "to execute the warrant within a specified time no longer than 14 days" and (b) to "execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time . . . ." The government seeks permission to deploy the NIT at any time of day or night within 14 days of the date the warrant is authorized. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. The government also seeks to read any messages generated by the activating computer as a result of a NIT at any time of day or night during the execution of the warrant. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

22. The government does not currently know the exact configuration of the computer that may be used to access the target address. Variations in configuration, e.g., different operating systems, may require the government to send the target address more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the target address for up to 14 days after this warrant is authorized, until the NIT has returned the information authorized to be collected by this warrant.

23. To the extent that use of a NIT to obtain the information described herein can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary for the reasons described herein.

24. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

A. the use of multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 14 days from the date this Court issues the requested warrant;

B. the NIT may cause an activating computer – wherever located – to send to FBI, located in Quantico, Virginia, in the Eastern District of Virginia, and then be relayed to the investigators in the Western District of Texas, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;

C. that the government may receive and read, at any time of day or night, within 14 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by the FBI;

D. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days from the sending of the NIT unless notification is further delayed by court order.

E. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

25. I further request that this Application and the related documents be filed under seal. The information to be obtained is relevant to an on-going criminal investigation. Premature disclosure of this Application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of the technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

WHEREFORE, Affiant respectfully requests that a warrant described above be issued.

SA JUSTIN E. NOBLE

Subscribed and sworn to me before me
this 18TH day of December, 2012

MARK LANE
U.S. Magistrate Judge